CERIAS

The Center for Education and Research in Information Assurance and Security

DPFace: Formal Privacy for Facial Images

Tao Li, Rohan Ashok, Chris Clifton

Dept. of Computer Science, Purdue University

Overview

- Growing privacy concerns from surveillance and social media exposure;
- We provide the first formal privacy guarantee for facial images;
- Maintain image fidelity while providing rigorous math guarantee.

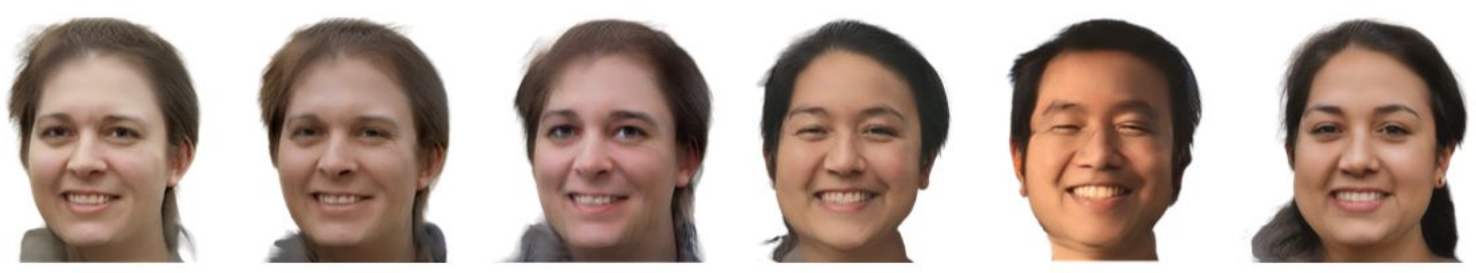

Fig. 1: Privatized Faces of the Authors.

Method

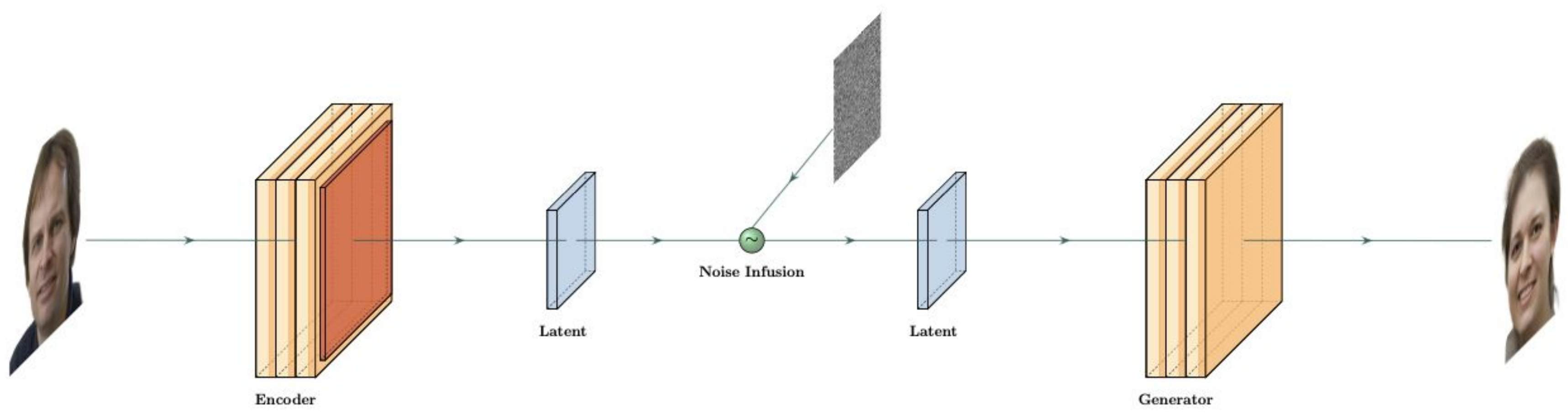

Fig. 2: Overview of the Image Privatization Framework.

- Step 1: From a public dataset D, select a cohort D_L based on predefined attributes (e.g., race, age, gender) and compute empirical sensitivity for each latent component z_j:

$$\Delta_j = \max_{i \in D_L}(z_{ij}) - \min_{i \in D_L}(z_{ij}).$$

- Step 2: Apply encoder ϕ to obtain latent representation $z=\phi(x;\theta_\phi)$; clip each component z_j to remain within the sensitivity bounds Δ_j:

$$z_j' = f_c(z_j; \Delta_j).$$

- Step 3: Infuse Laplace noise into z':

$$z'' = \mathcal{A}(z'; \Delta)$$

- Step 4: Re-clip z' within bounds Δ:

$$z''' = f_c(z''; \Delta)$$

  While not necessary for privacy, this reduces image distortion.
- Step 5: Generate the privatized image:

$$\hat{x} = \psi(z'''; \theta_\psi)$$

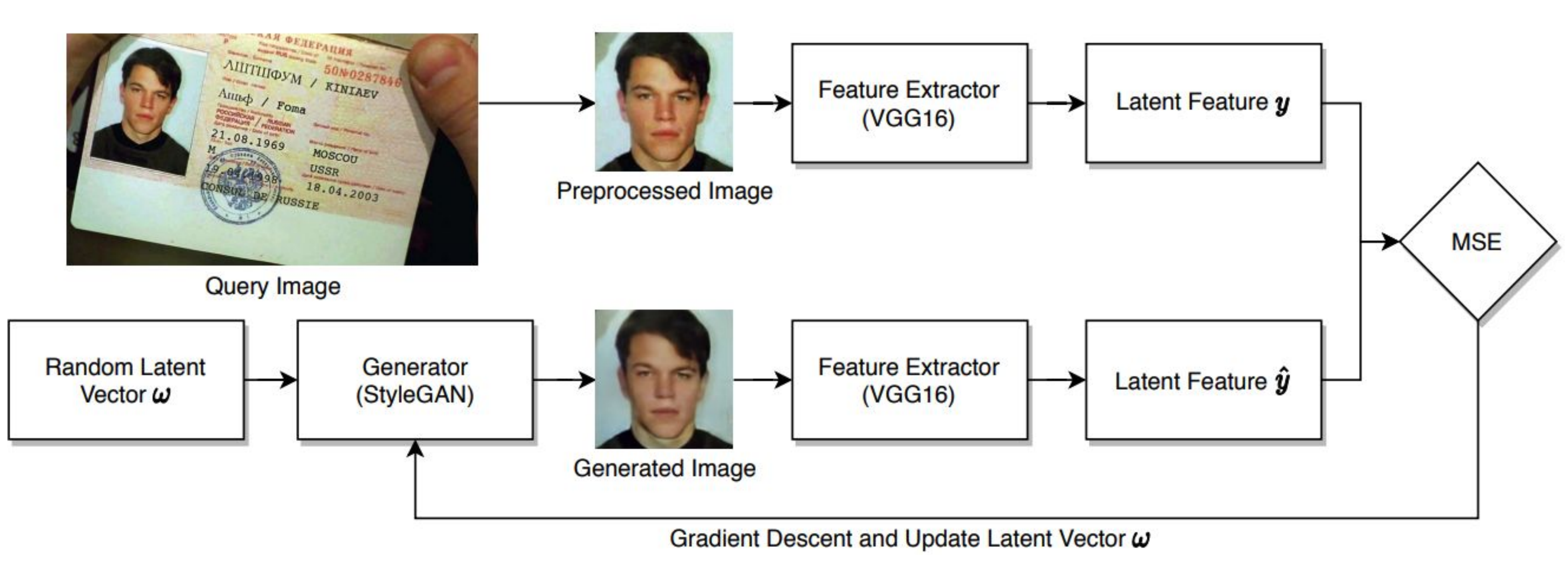

Fig 3: An Example of Image Encoding

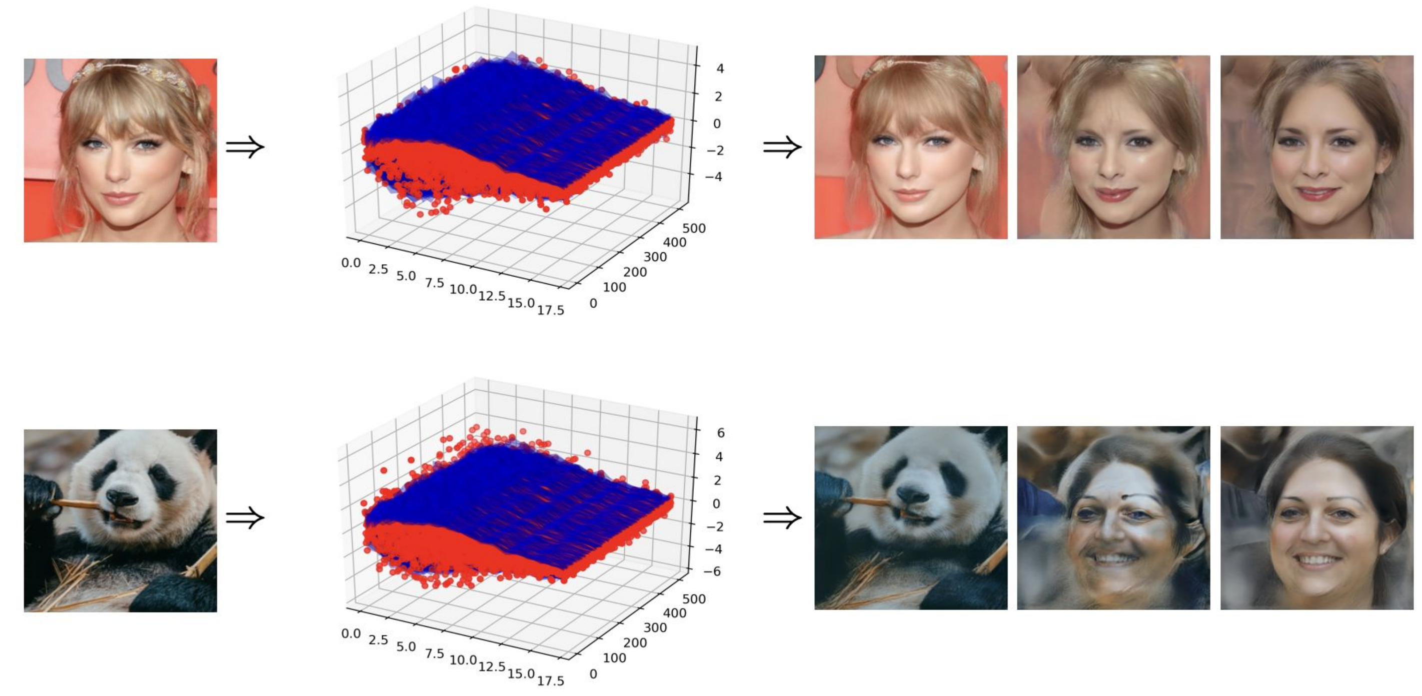

Fig. 4: The "Clipping" Mechanism.

Experimental Results

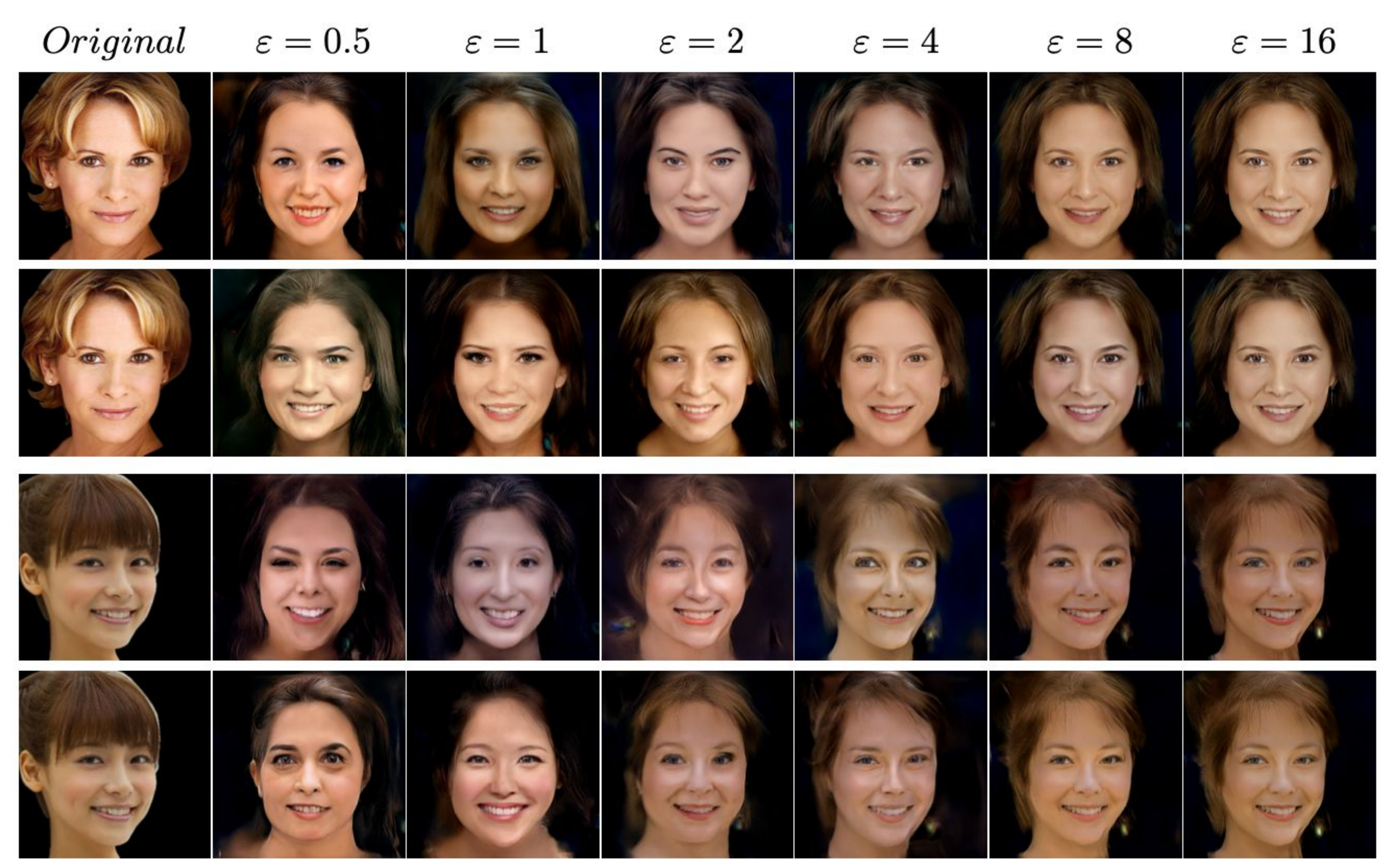

Fig. 5: Facial images with different privacy settings.

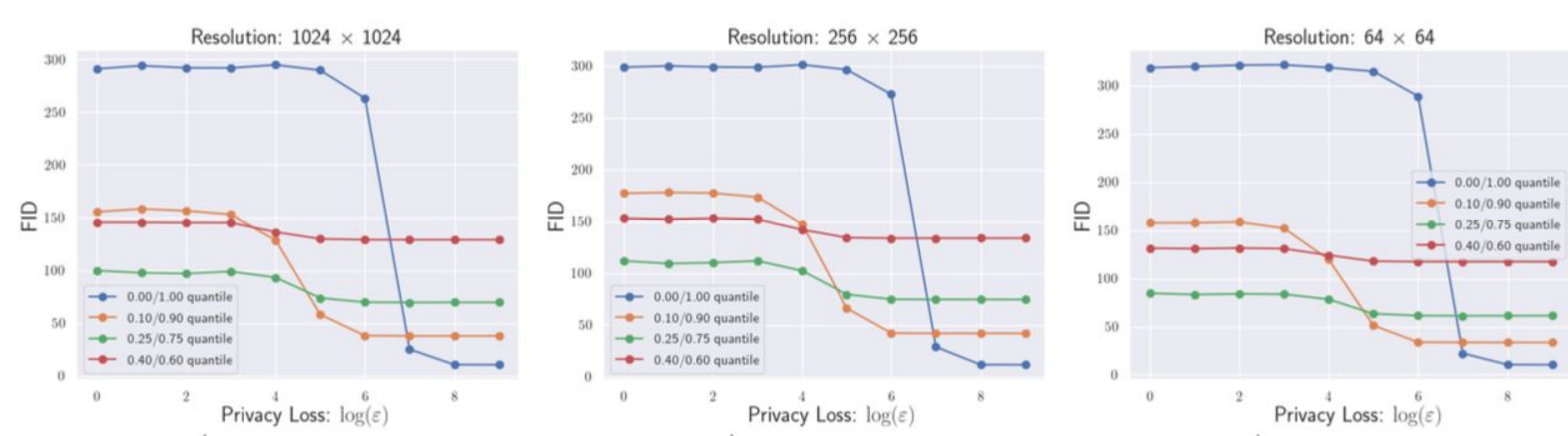

Fig. 6: Identity Distance and Privacy Loss.

Next: Formal Privacy for Gaits (Work in Progress)

- Gait is a unique biometric posing substantial privacy risks;
- Challenges: sequentiality, variability, spatiotemporal complexity.

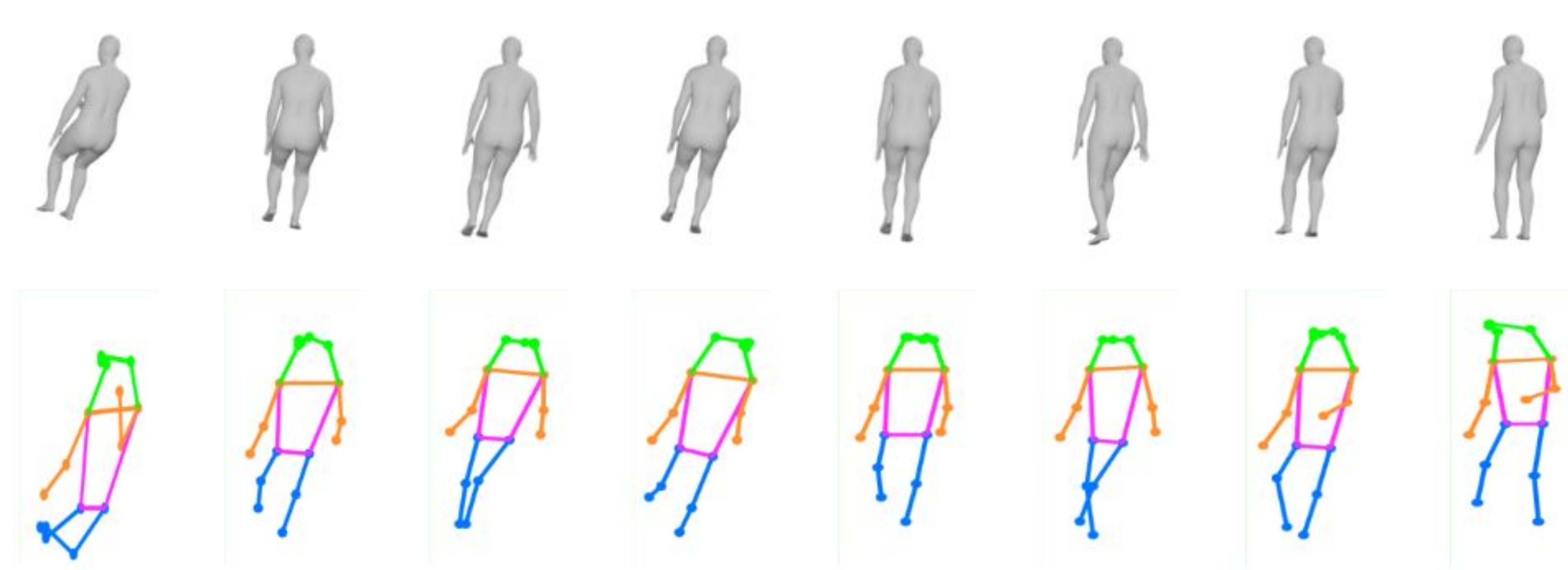

Fig. 7: 3D Mesh and Skeleton.